

CONFERENCE: WEDNESDAY, SEPT. 30, 2015
8 A.M.-4 P.M. (CHECK-IN BEGINS AT 7:30 A.M.)

NEW LOCATION! SOUTHEAST COMMUNITY COLLEGE, GYMNASIUM
8800 O ST., LINCOLN, NE

10th Annual

NEBRASKA

CYBER SECURITY CONFERENCE

cio.ne.gov/cyber-sec/events.html

STAYING AHEAD OF THE EVER-CHANGING CYBER THREATS
JOIN LEADING EXPERTS ON CYBER SECURITY.

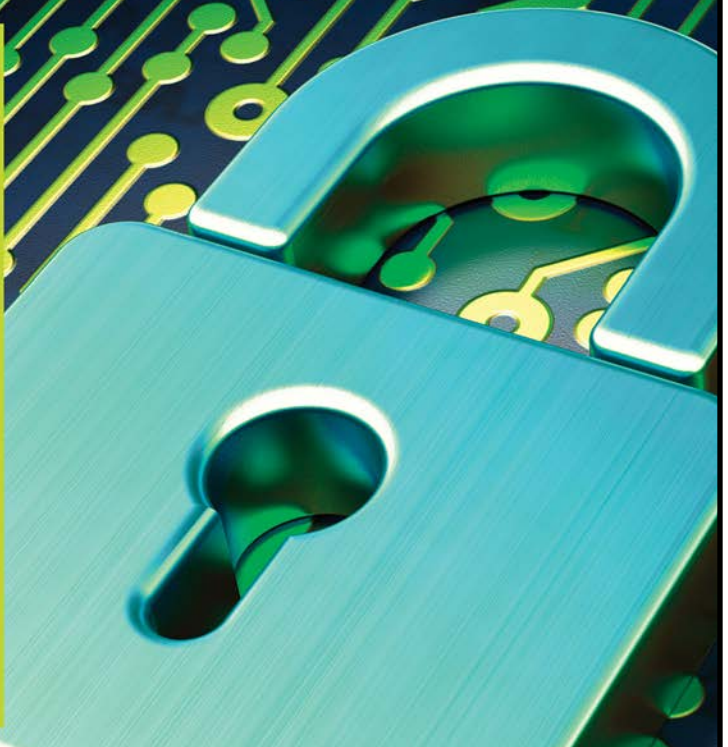
The Nebraska Cyber Security Conference is for security administrators and IT professionals including:

- Network Administrators
- System Administrators
- Information Security Professionals



This conference is a partnership between Southeast Community College and the state of Nebraska.

Southeast community college
www.southeast.edu/Training



In today's world, we rely on technology and the Internet for a variety of transactions, communication and information – at home, in school and at the workplace. While we are familiar with the myriad of conveniences

provided through Internet use, it is difficult to stay abreast of all the changes and the potential risks presented by the Internet. We are all “virtual neighbors” in cyberspace, and what we do, or don't do, can affect many others.

The Nebraska Cyber Security Conference will assist in raising our awareness of cyber security and help in protecting all of us in cyberspace. If we do our part individually, we can have a tremendous positive impact collectively on our state's cyber security.

This will be valuable time learning from skilled industry experts, including keynote presenter Rick Harris, Department of Homeland Security. The day will be filled with a variety of breakout sessions that will encompass different areas of information security and technology.

For more information: cio.ne.gov/cyber-sec/events.html



Richard “Rick” Harris

Policy, Plans and Strategy Office of Cybersecurity and Communications, U.S. Department of Homeland Security

Mr. Harris currently provides strategic advice and support to the Office of Cybersecurity and Communications where he has participated in numerous cyber and critical infrastructure cyber policy development and implementation processes. His previous role was the acting deputy director of the U.S. Computer Emergency Readiness Team where he led and coordinated initiatives to improve the nation's cybersecurity posture, promote cyber information sharing and manage cyber risks to the nation. Additionally, he supported monitoring and coordination functions for many of the activities under the Comprehensive National Cyber Initiative, a national program to increase the nation's cybersecurity posture and capabilities.

Mr. Harris began working with the National Cyber Security Division in 2004 as that organization was established. Joining US-CERT in 2007, he held several leadership roles. Mr. Harris created the Future Operations branch to conduct strategic and operational planning and coordination for the purpose of aligning the objectives of the US-CERT with the cybersecurity mission of DHS. He oversaw the planning, coordination and integration of the US-CERT's mission across the public and private sectors to protect cyberspace and coordinate cyber incident response. Additionally, he managed a \$24 million cybersecurity R&D Grant involving a consortium of more than 25 academic and research organizations. Mr. Harris also served on a 15-month detail assignment with the Office of the Director of National Intelligence's Joint Interagency Cyber Task Force where he was a senior portfolio manager for many of the CNCI programs.

Prior to joining DHS, Mr. Harris served with the United States Marine Corps from 1977 to 2004 before retiring as a colonel. He earned his BA degree in history and political science from Cornell College, Mt. Vernon, IA. Mr. Harris has two MAs: one in International Affairs from American University, Washington, DC and one in National Security and Strategic Studies from the Naval War College, Newport, RI. He has been awarded numerous military awards, including the Legion of Merit and Bronze Star Medal. Mr. Harris also was awarded a DHS Teamwork Award for his support to the CNCI, the Intelligence Community Meritorious Unit Award for his work at ODNI, and most recently an Intelligence Integration award for his efforts to coordinate interagency cybersecurity activities.



7:30 a.m.	Check-in	
8 a.m.	Opening Remarks from State of Nebraska Officials	
9:15 a.m.	Break	
9:30 a.m.	Breakout Session 1	<i>Active Shooter Training (Session 1 of 2)</i> , Shane Flynn <i>Combatting the Small Business Cyber Threat: Resources for Prevention & Recovery</i> , Kristen Judge <i>IRS Safeguards: Emerging Cyber Initiatives</i> , Steve Matteson <i>IoT: What is It & How to Prepare to Manage the Wave of Devices</i> , Jill Klein <i>Media Sanitization: Assessing Risk & Choosing A Solution</i> , Katie Fletcher <i>Protecting Crown Jewels: The People, The Data & The Applications</i> , Timothy Brown <i>Securing the Organization: An Effective Security Program</i> , Jim Coffman
10:30 a.m.	Break	
10:45 a.m.	Breakout Session 2	<i>Active Shooter Training (Session 2 of 2)</i> , Shane Flynn <i>PCI DSS 3.0 to 3.1: Minor Version, Major Change</i> , Jayne Friedland Holland <i>Cryptography & Its Future</i> , Abhishek Parakh <i>Consumer Privacy & Data Security: FTC Views & Enforcement Efforts</i> , Steve Baker <i>Information Security at UNMC</i> , Sharon Welna <i>Security as an Educational Enabler, Not an Inhibitor</i> , Todd Peterson <i>The Value & Process of Implementing a Security Vulnerability Program/Assessment</i> , Steve Hurst
Noon	Lunch (provided) & Keynote	Rick Harris, DHS
1:45 p.m.	Breakout Session 3	<i>OWASP: Soup to Nuts—Application Security</i> , Zac Fowler <i>10 Security Essential Practices Every CIO/CISO Needs to Know</i> , Jeff Jordan <i>Reducing One of the Major Pathways to a Cyber Attack</i> , David Saintsing <i>Cybersecurity in a Global Economy: How Do We Assure Growth While Protecting Our Digital Lives?</i> , Matt Morton <i>The Most-Traveled Route: Securing the Privileged Pathway</i> , Troy Brueckner <i>Under the Unfluence: The Dark Side of Influence</i> , Karla Carter <i>Cyber Warfare: Protect Against Attackers Hiding Amongst the Flock</i> , Anthony Lauro
2:45 p.m.	Break	
3 p.m.	Breakout Session 4	<i>The Cyber Threat Environment</i> , Ken Schmutz <i>Securing Your Identity Management Process</i> , David Saintsing <i>The State of Wireless Security</i> , Anthony Bolan <i>Mitigating Web Application Risks</i> , Michael Class <i>FireEye — Looking Inward: Changing Policy, Posture & Response Capabilities to Respond to Today's State Government Threat</i> , Thomas MacLellan <i>Everybody Has a Plan Until They Get Punched in the Mouth</i> , Dan Kottman

10 Security Essential Practices Every CIO/CISO Needs to Know

Jeff Jordan, IBM



Protecting your organization's data and infrastructure begins with a focus on effective security management: framing a management system around core practices and establishing a structure that allows the mapping of security initiatives to executive-level language. This systematic approach to security can help you better optimize your resources and investments, protecting what is essential to your mission and defending your organization against evolving threats.

Active Shooter Training

Shane Flynn, Nebraska Information Analysis Center

Learn what to do in the event of an active shooter in two sessions.

Combatting the Small Business Cyber Threat: Resources for Prevention & Recovery

Kristin Judge, National Cyber Security Alliance, StaySafeOnline.org

Small and midsize businesses are on the target list for hackers. While the larger corporations can recover from a cyber attack, small businesses may not come back. Learn what the most common cyber threats are facing small businesses, how to assess and protect company assets, and how to recover from an attack.



NCSA, a 501(c)(3) founded in 2001, is a leading public-private partnership, working with the U.S. Department of Homeland Security, corporate sponsors and nonprofit collaborations to promote cyber security and privacy awareness everywhere.

The FTC is launching a Data Security program in September 2015 to help small businesses protect data from cyber threats. Some of that material is being incorporated into an NCSA small business workshop to be ready Oct. 1.

Consumer Privacy & Data Security: FTC Views & Enforcement Efforts

Steve Baker, Federal Trade Commission

What we know of the extent and costs of data breaches, FTC enforcement against breaches and some of the failures that cause breaches. This presentation also will offer some ideas on how to guard against breaches.

Cryptography & Its Future

Abhishek Parakh, University of Nebraska-Omaha



The talk will present the current state of cryptography and the challenges it faces in the coming decades.

The Cyber Threat Environment

Ken Schmutz, FBI

This presentation will review the current cyber threats faced by business in the United States. This includes threats from criminals, terrorists, hackers, and nation state actors from the FBI's point of view. Information also will be discussed regarding the ways in which systems are compromised and what we can do about it.

Cyber Warfare: Protect Against Attackers Hiding Amongst the Flock

Anthony Lauro, Akamai Technologies

Cyber-attacks have become more organized, advanced, persistent, and adaptive. It is imperative for government organizations to be prepared to meet these dire challenges, and still meet current user's demands and compliance requirements. This session will explore the tactics attackers use at the front lines of cyber warfare, as well as some of the best practices for shoring up defenses, and identifying the wolves among the sheep.

Cybersecurity in a Global Economy: How Do We Assure Growth While Protecting Our Digital Lives?

Matt Morton, University of Nebraska-Omaha



As our planet becomes increasingly linked globally and as we continue to rely more heavily on technology for all aspects of our lives (work, home and entertainment), one cannot help but wonder if we are indeed creating a dependency that could be exploited to gain further control over our lives and information. Historically, those that controlled ports, roads and pathways for commerce also have been able to propel themselves to power. In addition, these roads also propagated ideas and influence that shaped the world we live in today. Today the Internet is the digital culmination of the ultimate commerce and idea "freeway." How do we continue to grow and leverage technology to both improve our lives and our economy while still protecting our privacy? This lecture will provide a real-life history of the growth and merger of our online and physical lives and provide direct examples of strategies for dealing with these risks.

Everybody Has a Plan Until They Get Punched in the Mouth

Dan Kottman, Optiv Security



As consultants with Optiv Security's (formerly FishNet Security) Attack and Pen. Team, we've executed more than 100 offensive assessments to identify and measure risk. Although we've observed a number of trends, both positive and negative, among clients spanning all industry verticals, one thing is transcendent: organizational planning (e.g. incident response, policy, etc.) is merely theoretical until tested. Relying on the presenters' consulting experience as well as industry news, this presentation intends to use actual breaches to convey deficiencies and strengths as well as potential offensive techniques that can be used to confuse, delay, subvert, or stress typical response plans and execution. The discussion will include a variety of technical and non-technical content, case studies and attack scenarios that further demonstrate the points being made.

FireEye — Looking Inward: Changing Policy, Posture & Response Capabilities to Respond to Today's State Government Threat

Thomas MacLellan, FireEye



Over the last several years the threats and attacks against state and local governments and educational institutions have become more ubiquitous, clandestine and adaptive. Unfortunately, governments and education systems continue to struggle to keep pace. This presentation will provide an overview of the national policy landscape in the context of the current threat environment and will offer a series of strategic recommendations that can help to enhance the governance, posture and response capabilities of governments and educational systems. Among the issues to be addressed are the need for the development of more intrinsic capabilities within and among organizations; the need for a rethinking of resource allocation within states; the need for rethinking risk management practices; and the need for reframing cybersecurity from an information technology issue.

Information Security at UNMC

Sharon Welna, UNMC



The presentation will talk about UNMC and its approach to information security.

IoT: What is It & How to Prepare to Manage the Wave of Devices

Jill Klein, Sirius



Are you struggling with network bandwidth issues? Are you concerned about how to secure all the personal devices and new IoT devices that are soon to be a part of your responsibility? Consumer applications will drive the number of connected things, while the enterprise will account for most of the revenue, says Gartner. Manufacturing, utilities and transportation will be the top three verticals using IoT in 2015, but by 2020, the ranking will change with utilities in the No. 1 spot, manufacturing second and government third.

IRS Safeguards: Emerging Cyber Initiatives

Steve Matteson, Internal Revenue Service

Media Sanitization: Assessing Risk & Choosing A Solution

Katie Fletcher, Data Security, Inc.



This presentation will be a review of the risks of handling media, information classification, a review of media disposal regulation (commercial industry and government standards), disposal options, and will finish with a question-and-answer session.

Mitigating Web Application Risks

Michael Class, Qualys



Mitigating Web application security risks is often complicated. Multiple technologies, multiple stakeholders, narrow windows for application changes, and other factors can make the tasks seem both risky and daunting. It doesn't have to be; we'll show you how.

The Most-Traveled Route: Securing the Privileged Pathway

Troy Brueckner, CyberArk

With access to privileged accounts, external hackers or malicious insiders can go anywhere in your enterprise, sometimes for months before attacking. Reinforcing perimeters, securing databases, and encrypting data mean nothing once privileged accounts are compromised. What if you had a way to secure the one thing needed in every successful attack? ... to stop attacks before they start? ... to disrupt attacks that have already started?

OWASP: Soup to Nuts—Application Security

Zac Fowler, OWASP



Join us for an update on OWASP activities, how you can use OWASP's free resources for your company, get some tips and tricks learned from AppSec USA, and hear more about the OWASP Lincoln chapter.

PCI DSS 3.0 to 3.1: Minor Version, Major Change

**Jayne Friedland Holland,
NIC. Inc.**



PCI 3.0 is an effort to keep pace with the shifting world of credit card payment security and to keep the standards relevant to current challenges and opportunities. It's also a response to events that have taken place since the last DSS version, such as the numerous security events that hit major retailers and financial institutions that continue to make headlines.

Protecting Crown Jewels: The People, The Data & The Applications

Timothy Brown, Dell



Do you know what your crown jewels are? Do you know how to protect them? In this session we will discuss how to discover and evaluate your crown jewels. We will then discuss the best practices to protect them and how to react when something goes wrong.

Reducing One of the Major Pathways to a Cyber Attack

David Saintsing, AOS



Connecting to remote systems represents 47 percent of the pathways used by cyber criminals to compromise your systems. When connecting to remote systems, you don't have to compromise security for productivity, or vice versa. With Bomgar's solutions, each encrypted connection is outbound, allowing you to connect without VPN or firewall changes, maintaining your perimeter security. You also can leverage Active Directory and LDAPS to manage authentication, define permissions for teams and individuals and capture detailed audit logs and recordings of every access session. In this presentation, you will learn how Bomgar builds solutions with security in mind, helping you meet compliance regulations and protect valuable data and systems from internal and external threats.

Securing the Organization: An Effective Security Program

Jim Coffman, Dell



Today's threat actors are more persistent than ever. While anti-virus and firewalls are a good start, an effective information security program needs to be more sophisticated to protect your organization. During this session Jim Coffman, CISSP, will present how a strong security program can safeguard your digital assets from breaches, achieve compliance and the importance of incident response readiness.

Securing Your Identity Management Process

David Saintsing, AOS



This presentation will show you how an organization simplifies managing user access across the enterprise, making it possible to achieve sustainable access compliance by fully automating the monitoring, reporting, certification and remediation of user entitlements.

Security as an Educational Enabler, Not an Inhibitor

Todd Peterson, Dell



For years, security has been the practice of denial, restriction and limitation. Accelerate learning by turning that around and make security the practice of connecting, permitting, uniting and educating. Dell IAM solutions facilitate positive, agile outcomes by appropriately connecting your educators, staff, students, and alumni to your systems and data to speed processes, permitting the “good guys” in your organization to do the right things, uniting the right users with the right systems and data without security barriers slowing things down. IAM for the real world enables your organization to operate smarter and more efficiently while increasing your level of security and compliance.

The State of Wireless Security

*Anthony Bolan, University
of Nebraska-Omaha*



The presentation covers recent developments in the realm of wireless devices (802.11 and some general other radio) security. The main areas focused on are attacks on wireless networks, location tracking of individuals by cell phone or IoT devices using a distributed framework, and a basic introduction to software-defined radio.

This presentation was given at the June 2015 NEbraskaCERT Cybersecurity Forum and to two groups of high school students participating in an information security event as part of the UNO Peter Kiewit Institute's Techademy program.

Under the Unfluence: The Dark Side of Influence

Karla Carter, Bellevue University



Every single one of the recent breaches is due to the failure of the human element. This session talks about how malicious hackers influence, or in this case “unfluence,” their victims using manipulation and coercion. Security professionals need to understand how they can be vulnerable to the factors of influence, so they can detect, deter and prevent it. Additionally, attendees will learn the importance of human factors, psychology and leadership for security professionals. The speaker also will cover social engineering through examples, demonstrations and case studies to make sure you and your employees aren't under the unfluence. Learn how here.

The Value & Process of Implementing a Security Vulnerability Program/ Assessment

Steve Hurst, AT & T



Learn the importance of implementing a vulnerability program and identify areas of weakness to minimize risk and impacts of a security breach.

SPONSORS



Southeast community college

How to Register

1. Complete the non-credit registration form contained in this brochure. **Please print or type information on the registration form.**

NOTE for State of Nebraska Employees: Please register at www.cio.ne.gov/cyber-sec/events.html

2. SEND the form with payment: **Check** payable to SCC, or **credit card** number (Mastercard, American Express, Discover, or Visa) or a **letter of authorization on company letterhead** if your employer is paying the tuition.

MAIL TO:

Jack J. Huck Continuing Education Center
301 S. 68th Street Place, Lincoln, NE 68510

FAX TO:

402-437-2703

Confirmations are not mailed.

REGISTRATION FORM - NON-CREDIT COURSE

Southeast community college

Complete this form with payment information and send via FAX or mail to:

**Jack J. Huck Continuing Education Center
301 S. 68th St. Place, Lincoln, NE 68510
FAX: 402-437-2703**

Include credit card information or Letter of Authorization for third-party billing.
The College requires a student's Social Security number as a condition for enrollment. A student's Social Security number information constitutes an "educational record" under the Family Educational Rights and Privacy Act (FERPA). The College will be privileged to redisclose that information only with the consent of the student or in those very limited circumstances when consent is not required by FERPA.

PLEASE PRINT

2015 QUARTER

☒ SUMMER ☐ WINTER
☐ FALL ☐ SPRING

Social Security Number OR SCC Student ID Number	Name: Last	First	Middle Initial	Email Address
Residence Mailing Address		City	State	Zip
				County #
Race (select one or more): <input type="checkbox"/> White <input type="checkbox"/> Asian <input type="checkbox"/> Native Hawaiian or Other Pacific Islander <input type="checkbox"/> Black or African American <input type="checkbox"/> American Indian or Alaska Native	<input type="checkbox"/> Nebraska Resident <input type="checkbox"/> Non-Resident	Birth Date	Business Phone	Home Phone
	Gender: <input type="checkbox"/> Male <input type="checkbox"/> Female	Ethnicity (select one): <input type="checkbox"/> Hispanic or Latino <input type="checkbox"/> Not Hispanic or Latino	Employer	

Nebraska Cyber Security Conference

Wednesday, Sept. 30, 2015 • 8 a.m.-4 p.m.

(Check-in begins at 7:30 a.m.)

Southeast Community College, 8800 O St., Lincoln, NE

Course #: INFO-6240

☐ **Early-Bird Registration: \$79**
(postmarked by Aug. 21) (Sec. LNUA)

☐ **Regular Registration: \$99**
(postmarked after Aug. 21) (Sec. LNUB)

☐ **Student Registration: \$50**
(Student ID Required at Check-in) (Sec. LNUC)

☐ **I would like a vegetarian entree for lunch.**

☐ **I would like a gluten-free entree for lunch.**

SCC Staff Tuition Waiver _____

Total Due \$ _____

CHECK ONE TOPIC IN EACH SESSION YOU WANT TO ATTEND

Breakout Session 1

- ☐ Active Shooter Training (Session 1 of 2)
- ☐ Combatting the Small Business Cyber Threat: Resources for Prevention & Recovery
- ☐ IRS Safeguards: Emerging Cyber Initiatives
- ☐ IoT: What is It & How to Prepare to Manage the Wave of Devices
- ☐ Media Sanitization: Assessing Risk & Choosing A Solution
- ☐ Protecting Crown Jewels: The People, The Data & The Applications
- ☐ Securing the Organization: An Effective Security Program

Breakout Session 2

- ☐ Active Shooter Training (Session 2 of 2)
- ☐ PCI DSS 3.0 to 3.1: Minor Version, Major Change
- ☐ Cryptography & Its Future
- ☐ Consumer Privacy & Data Security: FTC Views & Enforcement Efforts
- ☐ Information Security at UNMC
- ☐ Security as an Educational Enabler, Not an Inhibitor
- ☐ The Value & Process of Implementing a Security Vulnerability Program/Assessment

Breakout Session 3

- ☐ OWASP: Soup to Nuts—Application Security
- ☐ 10 Security Essential Practices Every CIO/CISO Needs to Know
- ☐ Reducing One of the Major Pathways to a Cyber Attack
- ☐ Cybersecurity in a Global Economy: How Do We Assure Growth While Protecting Our Digital Lives?
- ☐ The Most-Traveled Route: Securing the Privileged Pathway
- ☐ Under the Unfluence: The Dark Side of Influence
- ☐ Cyber Warfare: Protect Against Attackers Hiding Amongst the Flock

Breakout Session 4

- ☐ The Cyber Threat Environment
- ☐ Securing Your Identity Management Process
- ☐ The State of Wireless Security
- ☐ Mitigating Web Application Risks
- ☐ FireEye — Looking Inward: Changing Policy, Posture & Response Capabilities to Respond to Today's State Government Threat
- ☐ Everybody Has a Plan Until They Get Punched in the Mouth

SIGNATURE

☐ Check ☐ Cash ☐ Mastercard ☐ AMEX ☐ Discover ☐ VISA V Code _____

Name as it appears on card: _____

Exp.Date _____ Credit card # _____

Billing agency (INCLUDE LETTER OF AUTHORIZATION ON COMPANY LETTERHEAD)

For the protection of your personal credit card information, do not email this form to SCC. If faxing, only use the fax number listed or verify with SCC before using another SCC fax number.

Submission of this form indicates that I understand: **1)** that my registration is complete and that I am accountable for the tuition and fees and subject to a grade in the courses listed; **2)** that should I officially drop, cancel, or withdraw, any refund in tuition will be determined by the date I submit my request to Continuing Education; **3)** that failure to attend a course does not constitute an official drop/withdrawal; **4)** the personal information contained herein is correct as shown; and **5)** any changes in SSN, legal name, address, residency, etc. must follow the College procedures in the Student Handbook and College Catalog. It is the policy of SCC to provide equal opportunity and nondiscrimination in all admission, attendance, and employment matters to all persons without regard to race, color, religion, sex, age, marital status, national origin, ethnicity, veteran status, sexual orientation, disability, or other factors prohibited by law or College policy. Inquiries concerning the application of SCC's policies on equal opportunity and nondiscrimination should be directed to the Vice President for Access/Equity/Diversity, SCC Area Office, 301 S. 68th Street Place, Lincoln, NE 68510, 402-323-3412, FAX 402-323-3420, or jsoto@southeast.edu.

FOR OFFICE USE ONLY

ID# _____

DE _____